



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/751,539	01/06/2004	Gregory Sidebottom	0023-0180	3312
44987 7590 10/24/2008 HARRITY & HARRITY, LLP 11350 Random Hills Road SUITE 600 FAIRFAX, VA 22030				
EXAMINER				
SOL, ANTHONY M				
ART UNIT		PAPER NUMBER		
2419				
MAIL DATE		DELIVERY MODE		
10/24/2008		PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/751,539

Applicant(s)

SIDEBOTTOM ET AL.

Examiner

ANTHONY SOL

Art Unit

2419

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 6/5/2008.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,2,8-12,16,18,20-24,26-29,31 and 33-35 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,2,8-12,16,18,20-24,26-29,31 and 33-35 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

- In view of the Appeal Brief filed on 6/5/2008, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below.

- Claims 1, 2, 8-12, 16, 18, 20-24, 26-29, 31, and 33-35 remain pending.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1, 8-12, 16, 20-24, 26-29, 31, and 33-35 are rejected under 35

U.S.C. 102(e) as being anticipated by Pub. No. US 2005/0073982 A1 ("Corneille").

Regarding claim 1,

Corneille shows in fig. 1 firewall 124 (claimed extensible set of services) in customer network 114, which contains the second entity 5000.

Regarding claim 8,

Corneille discloses that the first entity 102 corresponds to a business partner system (para. 13, *It provides a **company** with wireless personal information management (PIM) functionality over general packet radio services (GPRS) or UMTS networks to end-users via a secure connection through a connector gateway system*) and the second entity corresponds to a service activation component 5000, the service activation component provides the service to a customer associated with the business partner system, the business partner system generates the message requesting service for the customer; and wherein the first interface module is further configured to: authenticate the business partner system based, at least in part, on information included in the message (para. 13, *The mobile provisioning tool system interfaces allow users to*

*provision mobile devices and manage mobile services, **customers**, end-users, and **authorizations**; para. 155, After querying the active directory 108, the following checks may be performed: a password check, a check of the expiration date of the account and a check to see if the account is blocked. If these checks are successful, the mobile provisioning tool system 103 may lookup what **authorization rights can be assigned** to the user (security group). Security groups will be maintained in the active directory 108. Based on the security group, the user will be granted access to only the data and functionality that he/she is authorized to access. So, customer users will not have access to other customer's data. Consequently, CRM Representatives will not have access to all of the functionality provided to Supervisors (Administrators). Although not illustrated, if any of the security checks above fail or a cancel button is selected, an "Access Denied" screen or page will be generated).*

Regarding claim 9,

Corneille shows in figs. 2-36 that the first entity 102 includes a plurality of service activation components (see numerous screen layouts of figs. 2-36); and wherein the system further comprises: a second entity locator configured to obtain information associated with the service activation components; and wherein the second interface module is further configured to: contact the second entity locator to identify one of the service activation components from which to request performance of the service (paras. 367-371, *the service table 5006 stores the services provisioned for each respective user. When a mobile network session is created for a user, the user's rows in this table*

will be inserted in a session lightweight directory access protocol (LDAP). The server table 5008 stores specific details about how the connector gateway application will connect to each customer server 5000 that will provide a service to the mobile device 102. When the connector gateway application is started, the server table 5008 is loaded into a memory location on the connector gateway server 104 and will be read to determine the customer server 5000 details when a connection will be made between a mobile device 102 and remote customer server 5000).

Regarding claims 10 and 21,

Corneille discloses that the message includes a subscriber identifier that identifies a subscriber on whose behalf the service is being requested (para. 371, *source IP on the request packet*); and wherein the second entity locator is configured to map the subscriber identifier to the identified one of the service activation components (paras. 367-371, *the service table 5006 stores the services provisioned for each respective user. When a mobile network session is created for a user, the user's rows in this table will be inserted in a session lightweight directory access protocol (LDAP). The server table 5008 stores specific details about how the connector gateway application will connect to each customer server 5000 that will provide a service to the mobile device 102. When the connector gateway application is started, the server table 5008 is loaded into a memory location on the connector gateway server 104 and will be read to determine the customer server 5000 details when a connection will be made between a mobile device 102 and remote customer server 5000).*

Regarding claim 11,

Corneille discloses that the connector gateway 104 may use Internet security server applications that provide firewall services for enterprise networks. For example, the connector gateway 104 may be built on top of Microsoft's Internet Security Acceleration (ISA) 2000 Server software, which provides firewall services for enterprise networks. ISA Server, an extensible platform that provides security, hardware redundancy, and load balancing and may have a comprehensive standard delivery kit (para. 352).

Regarding claims 12 and 22,

Corneille discloses that the connector gateway 104 may use Internet security server applications that provide firewall services for enterprise networks. For example, the connector gateway 104 may be built on top of Microsoft's Internet Security Acceleration (ISA) 2000 Server software, which provides firewall services for enterprise networks. ISA Server, an extensible platform that provides security, hardware redundancy, and load balancing and may have a comprehensive standard delivery kit (para. 352).

Regarding claims 16, 23, 24, 31, 33, 34, and 35,

Cornille shows in fig. 50 a service gateway 104 in communication with a first entity 102 and a second entity 5000, the service gateway comprising: a first interface module to receive, from the first entity, a message requesting performance of a service (para. 241, *During operation, the connector gateway 104 receives a request for a business service (such as Exchange) from an end user*) in an extensible set of services offered by the second entity (para. 352, *The connector gateway 104 may use Internet security server applications that provide firewall services for enterprise networks. For example, the connector gateway 104 may be built on top of Microsoft's Internet Security Acceleration (ISA) 2000 Server software, which provides firewall services for enterprise networks. ISA Server is an extensible platform that provides security, hardware redundancy, and load balancing and may have a comprehensive standard delivery kit;* para. 132, *A plurality of firewalls 124 may also be included on the carrier network 110 and the customer network 114 to provide additional security;* Note that the customer network 114 contains the second entity 5000. Therefore, second entity 5000 provides extensible set of services. See also para. 31), the message including a service name that corresponds to the service (para. 241, *receives a request for a business service (such as Exchange)*) and an argument that includes data useful in performing the service (para. 371, *To determine the customer server 5000, the session table 5010 is queried using the **source IP on the request packet** of the mobile device 102 to get the MSISDN*); an access control module to: make a first determination of whether the first entity is permitted to request performance of the service corresponding to the service name (para. 14, *The mobile provisioning tool system **provides security to prevent***

users from accessing accounts or services other than their own. *Users will access the system using credentials stored in an Active Directory (AD), which will restrict the user's access to data relevant only to the business roles they are authorized to use;* para. 33, *DNS communication requests are routed to the connector gateway, which determines if the user is authorized to access the requested service), make a second determination of whether the argument is permitted to be provided by the first entity, and make a third determination of whether the argument is permitted to be requested for the service corresponding to the service name (Note that the following italicized portion of paragraph 129 meets both limitation of **second determination and third determination**, The connector gateway 104 may also provide several technical benefits. It can integrate with RADIUS session LDAP to **control access based on device IP. Service access control** may be based on a user profile stored in a secure SQL database, **which prevents company A user from getting access to company B Server)**(Note: Thus, a source IP (claimed argument) will have to be determined if it correspond to a company A user (claimed first entity) in a SQL database before a requested service is granted); and a second interface module to selectively request performance of the service by the second entity based, at least in part, on results of the first, second, and third determinations of the access control module (para. 357, *The connector gateway 104 works by listening for requests from mobile devices 102. When a request is received from the mobile device 102, the connector gateway 104 performs a lookup to determine which customer server 5000 the connector gateway 104 should contact to complete the connection).**

Regarding claim 20,

Corneille discloses that the mobile provisioning tool system interfaces allow users to provision mobile devices and manage mobile services, **customers**, end-users, and **authorizations** (para. 13). Corneille further discloses that after querying the active directory 108, the following checks may be performed: a password check, a check of the expiration date of the account and a check to see if the account is blocked. If these checks are successful, the mobile provisioning tool system 103 may lookup what **authorization rights can be assigned** to the user (security group). Security groups will be maintained in the active directory 108. Based on the security group, the user will be granted access to only the data and functionality that he/she is authorized to access. So, customer users will not have access to other customer's data. Consequently, CRM Representatives will not have access to all of the functionality provided to Supervisors (Administrators). Although not illustrated, if any of the security checks above fail or a cancel button is selected, an "Access Denied" screen or page will be generated (para. 155).

Regarding claim 26,

Corneille shows in fig. 1 a service activation component 5000 configured to provide the services to the subscribers 102; and a service gateway 104 configured to act as a single point of contact between the retailer systems 102 and the service activation component 5000, the service gateway 104 providing controlled access, by the

retailer systems 102, to the services provided by the service activation component 5000, the service gateway 104 permitting each of the retailer systems 102 access to a subset of the services provided by the service activation component 5000 via the controlled access, the service gateway comprising: a first interface module to receive, from one of the retailer systems 102, a message requesting performance of one of the services by the service activation component 5000 ((para. 241, *During operation, the connector gateway 104 receives a request for a business service (such as Exchange) from an end user*), the message including at least one argument that includes data useful for performing the one service (para. 371, *To determine the customer server 5000, the session table 5010 is queried using the **source IP on the request packet of the mobile device 102 to get the MSISDN***), an access control module to: make a first determination of whether the one retailer system is permitted to request performance of the one service (para. 14, *The mobile provisioning tool system **provides security to prevent users from accessing accounts or services other than their own. Users will access the system using credentials stored in an Active Directory (AD), which will restrict the user's access to data relevant only to the business roles they are authorized to use***; para. 33, *DNS communication requests are routed to the connector gateway, which determines if the user is authorized to access the requested service*), make a second determination of whether the at least one argument is permissible for the one retailer system, and make a third determination of whether the at least one argument is valid for the one service (Note that the following italicized portion of paragraph 129 meets both limitation of **second determination and third determination**, *The*

*connector gateway 104 may also provide several technical benefits. It can integrate with RADIUS session LDAP to **control access based on device IP. Service access control** may be based on a user profile stored in a secure SQL database, **which prevents company A user from getting access to company B Server**)(Note: Thus, a source IP (claimed argument) will have to be determined if it correspond to a company A user (claimed first entity) in a SQL database before a requested service is granted, and a second interface module to selectively interact with the service activation component based, at least in part, on the first, second, and third determinations of the access control module (para. 357, *The connector gateway 104 works by listening for requests from mobile devices 102. When a request is received from the mobile device 102, the connector gateway 104 performs a lookup to determine which customer server 5000 the connector gateway 104 should contact to complete the connection*).*

Regarding claim 27,

Cornille discloses a firewall service, which is a network service (para. 352).

Regarding claim 28,

Cornille discloses that the connector gateway 104 may use Internet security server applications that provide firewall services for enterprise networks. For example, the connector gateway 104 may be built on top of Microsoft's Internet Security Acceleration (ISA) 2000 Server software, which provides firewall services for enterprise networks. ISA Server is an extensible platform that provides security, hardware

redundancy, and load balancing and may have a comprehensive standard delivery kit (para. 352). Corneille further discloses that a plurality of firewalls 124 may also be included on the carrier network 110 and the customer network 114 to provide additional security (para. 132). Note that the customer network 114 contains the service activation component 5000. Therefore, service activation component 5000 provides extensible set of services. See also para. 31.

Regarding claim 29,

Corneille discloses that the service gateway 104 and the service activation component 500 in combination provide a common interface via which the retailer systems 102 request one or more of the services provided by the service activation component 5000, the combination exposing subsets of the common interface to each of the retailer systems by controlling access to the services by the retailer systems.

(para. 241, *During operation, the connector gateway 104 receives a request for a business service (such as Exchange) from an end user*; para. 371, *To determine the customer server 5000, the session table 5010 is queried using the source IP on the request packet of the mobile device 102 to get the MSISDN*).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and

the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 2 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Corneille in view of US 2003/0055968 A1 ("Hochmuth").

Regarding claims 2 and 18,

Corneille shows in fig. 50 an IPsec router. However, Corneille does not explicitly disclose that the activation component is configured to configure a router to deliver a service.

Hochmuth discloses reconfiguration may also involve steps such as, but not limited to, configuring network devices to move a port on which network resource 42 is connected from one cell to another, configuring a router's access control list (ACL) and/or other parameters (para. 44).

It would have been *prima facie* obvious to one of ordinary skill in the art at the time of the invention was made to modify the connector gateway system of Corneille to provide a capability to provide router configuration service as taught by Hochmuth. One skilled in the art would have been motivated to make the combination to permit or deny access to network resource 42 through any network connection, and/or configuring a firewall (Hochmuth, para. 44).

Response to Arguments

5. Applicant's arguments with respect to claims 1, 2, 8-12, 16, 18, 20-24, 26-29, 31, and 33-35 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ANTHONY SOL whose telephone number is (571)272-5949. The examiner can normally be reached on M-F 7:30am - 4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Wing Chan can be reached on (571) 272-7493. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Anthony Sol/
Examiner, Art Unit 2619
10/23/2008

/Wing F. Chan/
Supervisory Patent Examiner, Art Unit 2619
10/20/08